UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/030,255 | 01/09/2002 | Michel Hazard | T2146-907683 | 8944 |

181 7590 12/22/2004

MILES & STOCKBRIDGE PC
1751 PINNACLE DRIVE
SUITE 500
MCLEAN, VA 22102-3833

| EXAMINER | |
|---|---|
| NGUYEN, NAM V | |
| **ART UNIT** | **PAPER NUMBER** |
| 2635 | |

DATE MAILED: 12/22/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 10/030,255 | HAZARD, MICHEL | |
| | Examiner | Art Unit | |
| | Nam V Nguyen | 2635 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *22 April 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1 and 3-15* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1 and 3-15* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

## DETAILED ACTION

This communication is in response to applicant's response to an Amendment which is filed April 22, 2004.

An amendment to the claims 1-5, 9, 11-12 and 14 has been entered and made of record in the application of Hazard for a "method for authenticating a portable object, corresponding portable object, and apparatus therefor" filed January 9, 2002.

Claim 2 is cancelled.

Claims 1 and 3-15 are pending.

### *Response to Arguments*

In view of applicant's amendment to amend the abstract to overcome the proper content, therefore, examiner has withdrawn the objection.

Applicant's amendments to the rejected claims are insufficient to distinguish the claimed invention from the cited prior arts or overcome the rejection of said claims under 35 U.S.C § 102(b) as discussed below. Applicant's amendment and argument with respect to the pending claims 1, 9, 12 and 14, filed April 22, 2004, have been fully considered but they are not persuasive for at least the following reasons.

On page 9, third paragraph, Applicant's arguments with respect to the invention in Kruse et al. does not teach or suggest that the use of parts of any program codes stored on the portable object for use in the calculation of a result used in the authentication process is not persuasive.

As defined by claim 1, the customer chip card (KK) of Kruse et al. includes a protected storage a secret cipher (KPC) and an authentication algorithm one-way function (f). The customer chip card (KK) includes a program authentication code PAC which then calculated with the assistance of this authentication algorithm (f) and of the secret cipher KPC from the program data. In order to prevent listening-in attacks and manipulations by learning the program authentication code PAC, a dynamic program check is executed with the assistance of a random number v. The random number v is generated in the customer card KK and is also forwarded to the customer terminal KT. Dependent on the random number v, a data block (Pv) is then selected with the assistance of the selection module SEL from the sensitive program parts P, both in the customer card KK. The random number generator for selecting parts of said a proper program (P) from said data memory in said customer card (KK). The afore-mentioned calculation of the program authentication code therefore ensues on the basis of this selected data block (Pv) according to the relationship: PACv = f (KPC:Pv) (column 2 lines 35 to 59; see Figures 1-2). Clearly, one skilled in the art understands that the customer card includes means for calculating an authentication code (PACv) from the stored program parts (Pv) with the assistance of an authentication algorithm (f) and using a secret cipher (KPC); and a comparison means (COMP) on said customer card (KK), for comparing the authentication code (PACv) calculated in the customer card (KK) for identity.

Furthermore, Kruse et al. disclose that a customer card (KK) is comprised in depositing the secret cipher KPC in a protected, programmable read-only memory or the cipher KPC is read from a specific chip card into the write-read memory of the customer terminal via the card reader of the customer terminal KT. A one-way function expediently comes into consideration as authentication algorithm f. At any rate, it should have so little complexity that it can be relatively easily implemented in a chip card. A number of possibilities are conceivable for the selection of a data block Pv from the sensitive program data P with the assistance of the random number v. For example, every Kth bit/byte can be selected from the program data P, whereby k is fixed and the random number v determines where the selection should be begun. Or, k=v applies and the start ensues with the first bit/byte of the program data P. However, the random number v, for example, can also initialize a further random number generator as a start value, with the output signals of this further random number generator determining the bits/bytes for the selected data block Pv. The stored program part P can also be card-specific so that an excessive amount of memory capacity is not used in the customer card KK for storing the sensitive program data. Checking all of the sensitive program part P is nonetheless guaranteed on the basis of the totality of cards (column 3 lines 2 to 44). Clearly, one skilled in the art understands that the customer chip card (KK) executes a calculation of a result by applying to said one-way authentication algorithm function (f) at least part (i.e. individual program parts (Pv) of said a proper program (P).

Therefore, Kruse et al. disclose that the use of parts of any program codes stored on the portable object for use in the calculation of a result used in the authentication process. The

examiner maintains that the references cited and applied in the last office actions for the rejection of the claims are maintained in this office action.

### *Claim Rejections - 35 USC § 102*

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1, 3-4, 9-10 and 12-15 are rejected under 35 U.S.C. 102(b) as being anticipated by Kruse et al. (US# 4,786,790).

Referring to claims 1, 9, 12 and 14, Kruse et al. disclose a data exchange system with authentication code comparator as recited in claims 1, 9, 12 and 14. See Figures 1-2 and respective portions of the apparatus and method.

Kruse et al. disclose a method for authenticating a portable object (KK) (i.e. a customer card) including information processing means (f) (i.e. a calculated program) and information storage means (P, Pv and KPC) (i.e. a memory having a proper program P, individual programming parts, and a secret cipher) (column 2 lines 20 to 66; column 3 line 27 to 32; see Figures 1-2), the information storage means (i.e. memory) containing at least one code (P) (i.e. a proper program) defining operation steps capable of being executed by the portable object (KK)

(column 2 lines 20 to 53), as well as a one-way function (f) (i.e. an authentication algorithm) (column 2 line 54 to column 3 line 13), comprising:

sending the portable object (KK) an order for executing a calculation of a result by applying to said one-way function (f) (i.e. an authentication algorithm) at least part (i.e. a selection of individual program parts (Pv) of said code (P) (i.e. a proper program) (column 2 lines 20 to 54; column 3 line 27 to 32; see Figures 1-2); and

entering said result (i.e. an output of a calculated program) into the implementation of a given operation, said operation being performed successfully only when the portable object (KK) is authentic (column 2 lines 55 to column 3 line 44; see Figures 1-2).

Referring to claim 3, Kruse et al. disclose a method according to claim 1, wherein said operation comprises a decryption operation, said result making it possible to produce an associated decryption key (column 2 lines 60 to column 3 line 9; see Figures 1-2).

Referring to claims 4, 10, 13 and 15, Kruse et al. disclose a method according to claims 2, 9, 12 and 14, wherein said part of said code (i.e. an individual program part) used in the calculation, comprises a machine code (i.e. programming code) (column 2 lines 20 to 66).

### *Claim Rejections - 35 USC § 103*

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person

having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 5, 8 and 11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kruse et al. (US# 4,786,790) as applied to claim 1 above, and in view of Anders et al. (US# 4,656,463).

Referring to claims 5 and 11, Kruse et al. disclose a method according to claims 1 and 9, however, Kruse et al. did not explicitly disclose further comprising wherein the portable object contains a real code that defines operations designed to be executed by the portable object, and a dummy code that defines operations not designed to be executed by the portable object, said code used in the calculation of a result comprising a dummy code.

In the same field of endeavor of access communication system, Anders et al. teach that the portable object (182) (i.e. an active transceiver) contains a real code (i.e. programming codes) defining operations designed to be executed by the portable object (column 12 lines 51 to column 13 line52; see Figure 13), and a dummy code (i.e. uncoded sectors) defining operations not designed to be executed by the portable object (182), said code (i.e. programming codes) used in the calculation of a result comprising a dummy code (uncoded sectors) (column 42 lines 43 to 59; see Figure 33) in order to obtain the best individual codes necessary for the operation of each individual system.

One of ordinary skilled in the art recognizes the need to generate programming codes of a tag having a particular code is not used with an uncoded sector of Anders et al. in a program authentication codes of a customer card of Kruse et al. because Kruse et al. suggest it is desired to provide that programming secret code in a protected, programmable read only memory from a

specific chip card (column 2 line 60 to column 3 line 9) and Anders et al. teach that an individual codes for the operation of each system is filled with a dummy code in an allocated area if an individual codes is not used in a particular system in order to increase the difficulty of decoding the source code. Therefore, it would have been obvious to a person of ordinary skill in the art at the time of the invention was made to generate programming codes of a tag having a particular code is not used with an uncoded sector of Anders et al. in a program authentication codes of a customer card of Kruse et al. with the motivation for doing so would have been to provide more secure method for authorization of a user.

Referring to claim 8, Kruse et al. in view of Anders et al. disclose a method according to claim 1, Anders et al. disclose wherein said code comprises a set of binary words, said code used in the calculation being defined by a subset of said binary words comprising binary words distributed in the information storage means at a determined pitch, said pitch being sent to the portable object (column 14 lines 7 to 36).

Claim 6 is rejected under 35 U.S.C. 103(a) as being unpatentable over Kruse et al. (US# 4,786,790) as applied to claim 1 above, and in view of Camion et al. (US# 6,167,516).

Referring to claim 6, Kruse et al. disclose a method according to claim 1, however, Kruse et al. did not explicitly disclose further comprising repeatedly sending said order to the portable object during its life, prior to execution by the portable object of said operation steps.

In the same field of endeavor of authentication device, Camion et al. teach that repeatedly sending said order to the portable object (1) during its life, prior to execution by the portable object (1) of said operation steps (column 9 line 51 to 55; column 11 line 31 to 51; see Figures 3-6) in order to restart calculation and to proceed to a new extraction of a word from a memory.

At the time the invention, it would have been obvious to a person of ordinary skill in the art to recognize the need for repeatedly until proceed to a new extraction of a word from source memory in the method of verifying data exchange system with authentication code comparator of Kruse et al. because repeatedly verifying for authentication of customer card would improve the reliable and secure communication between a chip card and a terminal that has been shown to be desirable in the data exchange system of Kruse et al.

Claim 7 is rejected under 35 U.S.C. 103(a) as being unpatentable over Kruse et al. (US# 4,786,790) as applied to claim 1 above, and in view of Nolan (US# 4,896,261).

Referring to claim 7, Kruse et al. disclose a method according to claim 1, however, Kruse et al. did not explicitly disclose wherein said code used in the calculation is defined by a start address and an end address in the information storage means, and further including the step of sending said start and end addresses to the portable object.

In the same field of endeavor of authentication device, Nolan teaches that code (i.e. message) used in the calculation is defined by a start address and an end address in the information storage means (22) (i.e. memory), and further including the step of sending said start and end addresses to the portable object (15) (i.e. control module) (column 1 line 58 to

column 2 line 21; column 4 lines 45 to 63; column 5 lines 10 to 29; see Figures 1-2) in order to identify each message was sent to the processor.

At the time the invention, it would have been obvious to a person of ordinary skill in the art to recognize to have a message sent to the control module having a start and end message address in key code programmable read only memory to process an authentication code of Kruse et al. because having a start and end address would distinguish the message from other message in the memory in order to improve reliable and secure communication between a chip card and a terminal that has been shown to be desirable in the data exchange system of Kruse et al.

## *Conclusion*

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Nam V Nguyen whose telephone number is 703-305-3867. The examiner can normally be reached on Mon-Fri, 8:30AM - 5:00PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Michael Horabik can be reached on 703-305-4704. The fax phone numbers for the organization where this application or proceeding is assigned are 703-872-9314 for regular communications and 703-872-9314 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

Nam Nguyen
December 13, 2004

MICHAEL HORABIK
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2600